TACOMA SCHOOL DISTRICT NO. 10
Pierce County, Washington
September 1, 1994 Through August 31, 1995

Schedule Of Findings

1. <u>Data Processing Controls Should Be Improved</u>

    During our audit of the Tacoma School District's accounting records, we reviewed the electronic data processing controls. We noted the following internal control weaknesses in the district's data processing system.

    a. Access to production programs and files was inadequately controlled or protected against unauthorized use, damage, or modification. Thirty-five user accounts have master terminal operator capability. A master terminal operator can perform tasks that have a significant impact on security and control of CICS and on the integrity of data defined to CICS.

    b. The district had no computer security or access control policy.

    c. There was no quality assurance or internal audit function reviewing the operations of data processing and, on a continuing basis, evaluating the effectiveness of existing controls.

    The lack of a coherent security administration plan has hampered the ability of the Management Information Services (MIS) department to implement adequate control procedures. The district's internal audit department has not performed a review of the DP operations. An internal audit is a managerial control which functions by measuring and evaluating the effectiveness of other controls.

    Access controls are designed to limit access to documentation, files, and programs. A weakness in or lack of such controls increases the opportunity for unauthorized modification to files and programs as well as misuse of the computer hardware. Proper access controls will assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation of data files, unauthorized or incorrect use of computer programs, or improper use of computer equipment.

    <u>We recommend</u> that written procedures, policies, and standards be established for the security system. Management should consider steps to ensure that all data processing access and security functions are being addressed in the new procedures.